Cyber Security and ICT Acceptable Use Policy

A Statement of Policy

Presented at Audit Finance & Risk…….Summer 2024

Ratified by Board of Trustees …Summer 2024

Reviewed Bi-annually

Next review due – Summer 2026

Responsible Officer: COO

Frequency of Review: upon significant change or every 24 months

Statutory

Amendments

Contents

Policy Statement

Any reference to 'the Trust' from here on refers to the Penk Valley Academy Trust. This policy is intended to provide a framework for such use of the Trust's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to. This policy applies to any users who have access to the Trust's ICT network but does not form part of any contract and can be varied from time to time, in order to comply with legal and policy requirements and in consultation with the appropriate bodies.

Users of the Trust's devices are bound by this policy. The Trust seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching ad innovation to the highest possible standards. This also requires appropriate and legal use of technologies and facilities made available to users of the Trust.

Penk Valley Academy Trust (referred to from here on as 'the Trust') is committed to promoting and facilitating the positive and extensive use of information technology in the interests of support

This Policy will be reviewed in the event of any significant change.

1. Scope

This Policy applies to all employees, volunteers, temporary staff, contractors, consultants and other workers at Penk Valley Trust. This policy applies to all services, systems and equipment that is owned or leased by the trust.

In association with this document elements of ICT may have its own policy with further in depth details such as mobile devices, remote working and BYOD (bring your own device), see item 12 related document's location.

The ICT Acceptable Use policy applies whether the systems are used outside office hours or outside of the workplace.

2. Reporting ICT Security incidents

Cyber security training is provided and is compulsory for all staff.

https://forms.office.com/r/iKev5761JH

If you become aware of a possible or suspected ICT security-related issue, whether it relates to a problem with a computer or an individual's actions then please report it immediately and in confidence to the trust ICT team and if appropriate to your Line Manager.

The ICT Helpdesk will instruct you on the correct procedures which you must undertake immediately to preserve the incident scene. If it is a virus-related incident, then see section 5 below for instructions. ICT will advise on how to proceed with the incident, do not touch or use the device until you have spoken with ICT.

The incident scene must be constantly monitored and protected to safeguard evidence., ie do not leave the device unattended or turn off.

If you do not feel that you can report the issue to your Line Manager or if the issue is of a sensitive or confidential nature, then you can contact the Data Protection Officer on dpo@penkvalley.co.uk

3 General use and Ownership

3.1 Hardware

All assets issued to or used within the Trust / school are the property of Penk Valley Trust and must not be used by unauthorised persons including family members:

You must not

- Connect privately owned ICT hardware, to any ICT equipment without permission from the ICT team and following the BYOD policy
- Modify or expose the inner workings of or in any other way tamper with any item of ICT Hardware;
- Relocate any item of ICT Hardware, other than items such as laptop computers that are intended to be portable without first consulting the ICT team.

Only ICT or approved contractors can service, modify, add or remove components or in any other way alter the ICT equipment.

3.2 Software and Apps

Software and apps for the purposes of this policy have been split out as follows. Software installed on PC's, computers that require a third party package to be installed (traditional application install) and App's software on IOS, Android and Windows store software. Its important to note that all new software must have a valid reason be it for education or business use.

Software, that normally requires the installation of packaged installer and for the most part will require ICT support. Software MUST NOT be purchased or requested to be installed without the permission of the HT, ICT manager and COO or DPO. For the most part it would be expected that a project would be created to manage the install and safety of data and that this may take several weeks to complete depending on the complexity of the install and data access required. Please discuss with your line manager before agreeing to anything.

You must not

- make unauthorised copies of copyrighted software, except as permitted by law or the owner of the copyright;
- download or install software from the Internet including shareware, apps, music and other audio files, games and screensavers.

The ICT Helpdesk should be contacted if you have queries regarding the restrictions and to obtain assistance with the removal of unauthorised software and files.

Apps i.e. IOS, Android and Windows Stores, will for the most part does not require ICT involvement. Care must be taken to ensure the legitimacy of the APP, many apps are not based in the UK and it would be a breach of data protection to use such apps without the appropriate safeguards inplace. As app's are very easily installed, you agree that by choosing to install an APP you take on full responsibility and accountability for the security of the data used on the app.

If you have any queries concerning the use and licensing of software, then please contact the ICT team through the Helpdesk helpdesk@penkvalley.co.uk
If you have any queries about

Attention is needed for any data being sent to external companies to facilitate the use of software, please see the Data Protection Policy for more details on how and what data can be sent to third parties and what steps you must take prior to signing up.

4 Transfer of Storage of Data

All data you create with Trust equipment and systems remains the property of the Trust. Any transfer of data must be in line with the Trust GDPR policy.

You must

- keep all business-related data on either OneDrive or SharePoint not on the hard drive of your PC. Data that is stored on OneDrive/SharePoint is backed up;

- Ensure that you regularly check the files that you have stored on OneDrive/ SharePoint and delete those that are no longer required;

- Lock sensitive data away when not in use;

- ensure that sensitive data, both paper-based and electronic is disposed of properly. Shred hardcopies and destroy disks.

You must not

- Store personal data (non PVAT work) files on the trust network or storage media including the OneDrive;
- Attempt to access any data or programs within the network that you do not have authorisation or the explicit consent of the owner of the data or program to do so. If you intentionally access a computer system or information without permission, then you are breaking the law under the Computer Misuse Act 1990;

- Send business-related sensitive/personal information via e-mail externally without suitable security measures being applied. Further advice can be sought from the ICT Helpdesk.

5 Computer viruses

It is a crime to deliberately or recklessly introduce a computer virus, under the Computer Misuse Act 1990. You must not use our e-mail and internet facilities for

- intentionally accessing or transmitting computer viruses or other damaging software;
- intentionally accessing or transmitting information about or software designed for, creating computer viruses.

If you find a virus, or suspect that your PC has one, you must immediately disconnect from the network, stop using the computer and tell the ICT helpdesk.
You must always follow the instructions that the ICT Helpdesk Support Team give you about virus attacks.
You must ensure that the Windows Defender Protection on your equipment is not disabled.

6 Access to email and internet services

Our e-mail and internet facilities are for business use only and must not be used in registering for online shopping or information that is not work related. Access to specific non-business-related sites may be restricted during certain times of the day to prevent an adverse impact on business use.

If your mailbox reaches the limit mail can still be received but the ability to send messages will be suspended. Mail can only then be sent once the mailbox is reduced below the limit. For advice and further assistance contact the ICT Helpdesk.

All internet and e-mail activity is logged for audit and performance monitoring purposes and the account holder is responsible for all activity logged against that account.

You must not attempt to connect to the network using another users account details.

You must:

- use Ctrl-Alt-Del keys to lock your windows PC when leaving your desk or the equivalent on other devices such as Phones, tablets etc.

7 Office 365 and teams use

- Files must not be shared under an anyone can access setting.
- Teams Chat and Video will be recorded and retained for 1 year
- Conduct on Teams Chat must be professional.

8 Prohibited use

The following section details prohibited use both in business and personal use:

You must not use, or try to use, our email and internet facilities to create, distribute or display in any form any material that is or maybe considered to be illegal, offensive or unacceptable under our rules and policies. It is impossible to give a complete list of what is considered offensive or unacceptable, but the following are included (and in some cases may also be illegal). Anything that:

- is pornographic or obscene, or includes any form of sexually explicit humour;
- is intimidating, discriminatory (for example, racist, sexist or homophobic) or breaks our anti-harassment and equal opportunities policies in any other way;
- is defamatory, encourages violence or strong feelings;
- is hateful;
- is fraudulent;
- shows or encourages violence or criminal acts;
- may give Penk valley or any of our schools a bad name; or
- is a deliberate harmful attack on systems we use, own or manage.

You must not use or try to use our facilities for:

- time-wasting activities, such as chain letters, or for sending private emails to everyone on the global address list;
- buying personal goods online or use your network password on any website other than Office 365;
- on-line gambling;

- carrying out a personal business operation for profit or charity;

- accessing, without permission, any email that is intended for another user or an email account of another user.

Unless performing a legitimate test as part of your normal job function and with authorisation of senior management, you must not use or try to use our facilities for:

- accessing or transmitting information about, or software designed for, breaking through security controls on any system;

- breaking through security controls to gain access on any system.

9 Copyright

Copyright applies to most documents automatically and that if you break the copyright rules you may be committing a criminal offence. However, a large amount of copyright material is put onto the internet with the expectation that it will be copied and distributed. The only sensible approach is to consider whether the author or owner of what is being transmitted is likely to object. For example, you can normally pass on an email that contains Government advice, but you must get permission before you pass on an email containing some technical advice from a commercial consultant.

10 Confidential or sensitive information

Data Protection Act

You must not break the conditions of the Data Protection Act 1998 when you use the email services or the internet for transmitting information. Please see the GDPR Policy for guidelines.

Sending Confidential or Sensitive Information via Email

The internet email facility is not a secure way of transmitting confidential, sensitive or legally privileged information. Internet email is as insecure as a postcard that you send through the normal post. So, you must make sure that the internet email is suitable for transmitting the information. If you need to send information that is confidential, sensitive or legally privileged, e.g. Social Care and Health reports on vulnerable children or details of project tender submissions, take advice from the ICT team about special security measures (such as encryption) that you must use. If you allow anyone to see this type of information without permission, you may be breaking the law.

11 Monitoring and Recording

Network Monitoring

For security, capacity planning and network performance purposes, authorised individuals within the trust may monitor equipment, systems and network traffic at any time. Penk valley trust reserves the right to audit networks and systems on a periodic basis to ensure compliance with PVAT and school policies.

Email Monitoring

We have the right to monitor and inspect:

- any emails sent using our systems, both to internal and external addresses;
- any emails received using our systems;
- any material downloaded from the internet using our systems; and
- any electronic material stored on our systems.

We own our email system which means that we also own all copies of messages created, received or stored on the systems. This means that nothing will be private, even if marked as "private" and/or "confidential" or with any similar wording.

This monitoring will make sure that this policy is effective and that our users are keeping to it. It also makes sure that our computer systems are working properly.

Internet Usage Monitoring

We centrally record how our internet facilities are used. We regularly inspect the records to check for any access or attempted access to internet sites that are not allowed or may cause our systems to be damaged either physically or reputationally. We also monitor the records to make sure that our business is not affected by excessive personal internet use or by unauthorised internet use.

We have the right to monitor and inspect any internet use for any purpose we deem necessary. There can be no expectation that the use of our systems for looking at the internet sites will be private.

If you access a prohibited internet site unintentionally, you must break the connection immediately and report it to your Headteacher or Line Manager. If you do not do this, we may take action against you.

12 If You Break This Policy

If you break any of the rules on purpose, we may:

- withdraw your access to the email or internet facilities, temporarily or permanently;
- take disciplinary action against you (if you are staff);
- refer the matter to the appropriate ethics or standards committee (if you are an elected member);
- bring criminal proceedings against you, or ask the police or other relevant body to, if the matter is also a criminal offence; or
- do a combination of these things.

If you misuse our systems, we could take disciplinary action against you which may lead to you being dismissed. Serious cases will result in you being dismissed for gross misconduct.

If you try to damage, defeat or deceive one of our security facilities, we will take disciplinary action against you.

If you suspect someone has broken this policy, you must report this to your Line Manager. If a problem is discovered at an early stage, we can usually deal with it at a local level. However, if the case is more serious, the Line Manager will report it to their Line Manager. In certain circumstances, we may need to carry out an investigation and internal audit.

If you find or suspect anyone of using the computer system illegally or unethically, you should report it the Trust Data Protection Officer dpo@penkvalley.co.uk

13 Linked policy's

- GDPR Policy
- Privacy Policy
- Mobile Devices
- Remote working
- BYOD
- Cyber security training https://forms.office.com/r/iKev5761JH